UNITED STATES PATENT AND TRADEMARK OFFICE

11A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,579	10/09/2003	Yung Chang Liang	TRNDP011	9448

22434 7590 11/20/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2196	

DATE MAILED: 11/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	10/683,579	LIANG ET AL.	
	Examiner	Art Unit	
	Randal D. Moran	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 October 2003*.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-33* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *09 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a)☐ All b)☐ Some * c)☐ None of:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *3/01/2005 and 4/11/2005*.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The Information Disclosure Statement filed on March 1 2005 has been considered by the examiner.

2. The Information Disclosure Statement filed on April 11, 2005 has been considered by the examiner.

3. Claims 1-33 are pending in this application.

Specification

4. The disclosure is objected to because of the following informalities:

- [0022] line 4, "tier 2 switch 122" references tier 3 switch in Figure 1.
- [0022] line 5, "tier 3 switch 124" is not present in Figure 1.
- [0039] line 11, "a mode change command 506" is not present in Figure 5.
- [0041] line 6, "virus warning 508" is not present in Figure 5 or 6A.

Appropriate correction is required.

Claim Objections

5. The following claims are objected to for lack of antecedent basis.

a.) **Claim 1,** recites the limitation "the virus/monitor sensor" in line 5.

b.) **Claim 7** recites the limitation "the trash collector" in line 5.

c.) **Claim 9** recited the limitation "the copied data packet" in line 3.

d.) **Claim 13** recites the limitation "the traffic controller" in line 5.

e.) **Claims 15-** line 4, **19-** line 5, **and 20-** line 1, recites the limitation "the virus/worm analyzer."

f.) **Claim 22** recites the limitation "the filescan unit" in line 2.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 1, 6, 9, 10, 13, 14, 16, 17, 20, 21, 24, 27, 28, 31, and 32** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Considering **Claims 1-** lines 6-7, **13-** lines 4-6, **and 24-** lines 5-6, "the bandwidth of the network is substantially unaffected by the traffic controller during a virus/worm sensing operation." It is not clear how the sensing operation may/may not affect the bandwidth.

9. Considering **Claims 6-** lines 3 and 6, **9-** line 4, **10-** lines 3 and 6, **16-** line 5, **17-** lines 3 and 6, **20-** line 5, **21-** lines 3 and 6, **27-** line 5, **28-** lines 4 and 7, **31-** line 6, **and 32-** lines 4 and 7, it is unclear what is meant by the term "likely to." It is

unclear what criteria are used to determine if a protocol is likely to be infected rendering the claim vague and indefinite. It is interpreted to mean certain protocols will cause a packet to be flagged. This interpretation will be used for the remainder of the office action.

10. Considering **Claim 14-** line 2, "copying substantially all data packets." It is unclear in which mode this copying process is taking place.

Double Patenting

11. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

12. **Claims 1-33** are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-30 of copending **Application No. 10/683582,** herein after "582" in view of **Suuronen et al. (US 2003/0145228),** herein after "Suuronen".

This is a provisional obviousness-type double patenting rejection

13. **Claims 1, 13, and 24** of the instant application correspond to Claims 10, 20 and 30 of `582 respectively. The claims vary in breadth. Claims 10, 20 and 30 respectively of `582 claims all the limitations set forth in claims 1, 13, and 24 respectively of the instant application except for a traffic controller in communication with the network.

Suuronen discloses a traffic controller in communication with the network.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify `582 by a traffic controller as taught by Suuronen for the benefit of early packet classification so that it is possible to route real time traffic through a gateway which processes the data packets prior to testing with the virus scanning engine. The early classification improves the performance of the gateway (Suuronen [0007] lines 5-10).

14. **Claims 13-33** are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-14 of copending **Application No. 10/683873**, herein after "873". Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims in the instant application are a broader version of the claims in `873.

This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

15. **Claim 13** of the instant application corresponds to Claims 1 and 2 of `873. The claims vary in breadth. The instant application sets forth all the limitations of `873 as follows: during a virus/worm sensing operation, the bandwidth is substantially unaffected by the traffic controller by the network virus/worm sensor in a first mode wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic, only those data packets infected by the detected computer virus or computer worm are not returned to the network, which encompasses all the limitations of Claim 1 in `873. The limitation of switching when a computer virus or computer worm is detected to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network corresponds to Claim 2 of `873.

16. **Claims 14,15, 16, 17, and 18** of the instant application correspond to Claim 4, 5, 6, and 7 of `873 respectively.

17. **Claim 24** of the instant application corresponds to Claims 8 and 9 of `873. The claims vary in breadth. The instant application sets forth all the limitations of `873 as follows. Computer code for performing a virus/worm sensing operation, the bandwidth is substantially unaffected by the traffic controller by the network virus/worm sensor in a first mode wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic, only those data packets infected by the detected computer virus or computer worm are not returned to the network, which encompasses all the claim limitations of Claim 8 in `873. The limitation of switching when a computer virus or computer worm is detected to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network corresponds to Claim 9 of `873.

18. **Claims 25 and 26** of the instant application correspond to Claim 11 of `873.

19. **Claim 27, 28, 29, and 30** of the instant application correspond to Claims 12, 13, 14, and 10 of `873 respectively.

Claim Rejections - 35 USC § 102

20. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

21. **Claims 1, 2, 8, 12, 13, 23, and 24** are rejected under 35 U.S.C. 102(e) as being anticipated by **Suuronen et al. (US 2003/0145228)**, herein after "Suuronen".

22. Considering **Claim 1**, Suuronen discloses a network virus/worm monitor (abstract lines 3-6, Fig. 1, [0019] lines 2-7), comprising: a network virus/worm sensor (Fig. 1-item 22, [0021] lines 1-14); and a traffic controller in communication with the network (Fig. 1-item 14 and item 16, [0020] the combination of the Firewall and Packet Classification Database act as a traffic controller to determine which packets get transferred to the network and which packets get forwarded to the Virus Scanning Engine); virus/monitor sensor and the network operable in a number of modes (Fig 1, [0021] lines 1-14) wherein in a first mode the bandwidth of the network is substantially unaffected by the traffic controller during a virus/worm sensing operation by the network virus/worm sensor ([0007] lines 5-10, [0020] lines 2-9 being able to process packets in real time would mean that the bandwidth is unaffected by this process, in a first mode no virus is detected and all packets are returned directly to the network), wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic (Fig. 1-item 22 and item 24, page 4, left column, lines 33-34), the

virus/worm sensor causes the traffic controller to switch to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network (Fig. 1, page 4, left column, lines 11-15 packets that are discarded are not returned to the network).

23. Considering **Claim 13**, Suuronen discloses a method of managing network traffic by a network virus/worm monitor (abstract lines 3-6, Fig. 1, [0019] lines 2-7), having a network virus/worm sensor (Fig. 1-item 22, [0021] lines 1-14), comprising: during a virus/worm sensing operation, the bandwidth of the network is substantially unaffected by the traffic controller by the network virus/worm sensor in a first mode ([0007] lines 5-10, [0020] lines 2-9 being able to process packets in real time would mean that the bandwidth is unaffected by this process, in a first mode no virus is detected and all packets are returned directly to the network), wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic (Fig. 1-item 22 and item 24, page 4, left column, lines 33-34); and switching when a computer virus or computer worm is detected to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network (Fig. 1, page 4, left column, lines 11-15 packets that are discarded are not returned to the network).

24. Considering **Claim 24**, Suuronen discloses a computer program product (page 6, left column, lines 16-29) for managing network traffic by a network virus/worm monitor (abstract lines 3-6, Fig. 1, [0019] lines 2-7), having a network virus/worm sensor (Fig. 1-item 22, [0021] lines 1-14), comprising: computer code for performing a computer virus/worm sensing operation (page 6, left column, lines 16-29), the bandwidth of the network is substantially unaffected by the traffic controller by the network virus/worm sensor in a first mode ([0007] lines 5-10, [0020] lines 2-9 being able to process packets in real time would mean that the bandwidth is unaffected by this process, in a first mode no virus is detected and all packets are returned directly to the network), wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic (Fig. 1-item 22 and item 24, page 4, left column, lines 33-34); computer code for switching when a computer virus or computer worm is detected to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network; and computer readable medium for storing the computer code (Fig. 1, page 4 left column, lines 11-15 packets that are discarded are not returned to the network).

25. Considering **Claim 2**, Suuronen discloses those data packets deemed to be infected by the identified computer virus or computer worm are forwarded to a virus/worm analyzer unit coupled to the network computer virus/worm sensor ([0019] lines 27-32).

26. Considering **Claim 8**, Suuronen discloses in the second mode, only those original data packets included in the network traffic suspected of being infected by the detected computer virus or computer worm are forwarded by the traffic controller to the virus/worm analyzer unit ([0019] lines 27-32).

27. Considering **Claims 12 and 23**, Suuronen discloses the first mode is an inline mode ([0020] lines 2-9); and wherein the second mode is a standby mode ([0019] lines 27-32).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. **Claims 3-5, 9, 10, 14-16, 19-21, and 25-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Suuronen** in view of **Ontiveros et al. (US 2002/0107953),** herein after “Ontiveros”.

30. Considering **Claims 3, 14, and 25**, Suuronen does not disclose in the first mode, substantially all data packets included in the network traffic are copied by the traffic controller.

Ontiveros discloses in the first mode, substantially all data packets included in the network traffic are copied by the traffic controller ([0035] lines 1-3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Suuronen by copying all data packets included in the network traffic as taught by Ontiveros in order to maintain throughput of data traffic thereby increasing performance (Ontiveros [0035] lines 1-3).

31. Considering **Claims 4, 15, and 26**, the claims are rejected for the same reasons as claim 3, 14, and 25 above, Suuronen and Ontiveros disclose substantially all of the copied data packets are forwarded to the virus/worm analyzer unit (Suuronen- [0019] lines 27-32, Ontiveros- [0035] lines 1-3).

32. Considering **Claims 5, 16, and 27**, the claims are rejected for the same reasons as claim 3, 14, and 25 above, Suuronen and Ontiveros disclose the copied data packet is forwarded to a packet protocol determinator that determines if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm (Suuronen- [Fig 1-item 16, [0019] lines 7-14, Ontiveros [0035] lines 1-3).

33. Considering **Claim 9**, Suuronen and Ontiveros disclose the original data packet is forwarded to a packet protocol determinator that determines if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm (Suuronen- [Fig 1-16, [0019] lines 7-14, Ontiveros [00365] lines 1-3).

34. Considering **Claim 10,** Suuronen discloses a network interface arranged to return to the network traffic only those original data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm ([0019] lines 14-18), wherein the filescan unit receives and analyzes those original data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm ([0021] lines 1-14]).

35. Considering **Claim 19**, Suuronen discloses in the second mode, only those original data packets included in the network traffic suspected of being infected by the detected computer virus or computer worm are forwarded by the traffic controller to the virus/worm analyzer unit ([0019] lines 27-32).

36. Considering **Claim 20,** the claims are rejected for the same reasons as claim 3, 14, and 25 above, Suuronen and Ontiveros disclose the original data packet is forwarded to a packet protocol determinator that determines if the packet

protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm (Suuronen- [Fig 1-item 16, [0019] lines 7-14, Ontiveros- [0035] lines 1-3).

37. Considering **Claim 21**, Suuronen discloses a network interface arranged to return to the network traffic only those original data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm ([0019] lines 14-18), wherein the filescan unit receives and analyzes those original data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm ([0021] lines 1-14]).

38. **Claims 6, 17, and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Suuronen** in view of **Ontiveros** in further view of **Balissat et al. (US 2003/0191963)**, herein after "Balissat".

39. Considering **Claims 6, 17, and 28**, Suuronen and Ontiveros disclose a filescan unit arranged to receive and analyze those copied data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm (Suuronen- [0021] lines 1-14], Ontiveros- [0035] lines 1-3).

Suuronen and Ontiveros do not disclose a trash collector arranged to receive those copied data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm.

Balissat discloses a trash collector arranged to receive those copied data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm ([0096] lines 10-14).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Suuronen and Ontiveros by discarding the copied packets to a trash collector as taught by Balissat for the benefit of discarding the packets and not returning them to the network increasing storage space and efficiency.

40. **Claims 7, 18, 29-33** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Suuronen, Ontiveros and Balissat** in further view of **Wells (US 6,338,141).**

41. Considering **Claims 7, 18** and **29,** Suuronen, Ontiveros and Balissat discloses a virus/worm analyzer unit arranged to determine if those copied data packets received at the filescan unit are infected by the detected computer virus or computer worm (Suuronen- [0021] lines 1-14], Ontiveros- [0035] lines 1-3); wherein those packets determined not to be infected are forwarded to the trash collector (Balissat- [0096] lines 10-14);

Suuronen, Ontiveros and Balissat do not disclose a virus analysis unit arranged to analyze the infected copied data packets and a virus report module arranged to generate a virus report based upon the analysis.

Wells does disclose a virus analysis unit arranged to analyze the infected copied data packets (column 2 lines 47-53) and a virus report module arranged to generate a virus report based upon the analysis (column 2 lines 47-53 the output from the analysis-implementation that is used to update the virus detection database is a report).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Suuronen, Ontiveros, and Balissat by a virus analysis unit that generates a virus report as taught by Wells for the benefit of providing virus updates to the virus detection system (Wells- column 2 lines 50 –53).

42. Considering **Claim 30**, Suuronen discloses in the second mode, only those original data packets included in the network traffic suspected of being infected by the detected computer virus or computer worm are forwarded by the traffic controller to the virus/worm analyzer unit ([0019] lines 27-32).

43. Considering **Claim 31**, Suuronen and Ontiveros disclose the original data packet is forwarded to a packet protocol determinator that determines if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm (Suuronen- [Fig 1-item 16, [0019] lines 7-14, Ontiveros- [0035] lines 1-3).

44. Considering **Claim 32**, Suuronen discloses a network interface arranged to return to the network traffic only those original data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm ([0019] lines 14-18), wherein the filescan unit receives and analyzes those original data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm ([0021] lines 1-14]).

45. Considering **Claim 33**, Suuronen discloses the virus/worm analyzer unit determines if those original data packets received at the filescan unit are infected by the detected computer virus or computer worm ([0021] lines 7-14); wherein those packets determined not to be infected are forwarded to the network interface for return to the network traffic ([0021] lines 21-22).

Suuronen, Ontiveros, and Balissat do not disclose the virus analysis unit analyzes the infected original data packets and the virus report module generates a virus report based upon the analysis.

Wells does disclose the virus analysis unit analyzes the infected original data packets (column 2 lines 47-53) and the virus report module generates a virus report based upon the analysis (column 2 lines 47-53 the output from the analysis-implementation that is used to update the virus detection database is a report).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Suuronen, Ontiveros, and Balissat by a virus analysis unit that generates a virus report as taught by Wells for the benefit of providing virus updates to the virus detection system (Wells- column 2 lines 50–53).

46. **Claim 11 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Suuronen** in view of **Ontiveros** in further view of **Wells.**

47. Considering **Claims 11 and 22,** Suuronen discloses the virus/worm analyzer unit determines if those original data packets received at the filescan unit are infected by the detected computer virus or computer worm ([0021] lines 7-14); wherein those packets determined not to be infected are forwarded to the network interface for return to the network traffic ([0021] lines 21-22).

Suuronen and Ontiveros do not disclose the virus analysis unit analyzes the infected original data packets and the virus report module generates a virus report based upon the analysis.

Wells does disclose the virus analysis unit analyzes the infected original data packets (column 2 lines 47-53) and the virus report module generates a virus report based upon the analysis (column 2 lines 47-53 the output from the analysis-implementation that is used to update the virus detection database is a report).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Suuronen and

Ontiveros by a virus analysis unit that generates a virus report as taught by Wells for the benefit of providing virus updates to the virus detection system (Wells- column 2 lines 50–53).

Conclusion

48. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 5,889,943- e-mail virus detection and elimination.
- US 2002/0133586- copying data packets, related to Ontiveros application.
- US 6,480,471- discards copied packets.
- US 2004/0042418- discards duplicate and copied packets in a fault tolerant network.

49. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil El-Hady can be reached on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran

RDM

11/8/06

N. ElHady

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER